Efficient Identity-based Broadcast Encryption without Random Oracles

Liang Hu, Zheli Liu
Department of Computer Science and Technology, Jilin University, Changchun, China
Email: {hul, liuzheli}@jlu.edu.cn
Xiaochun Cheng
Department of Computer Communications, Middlesex University, London, England
Email: X.Cheng@mdx.ac.uk

***Abstract*— We propose a new efficient identity-based broadcast encryption scheme without random oracles and prove that it achieves selective identity, chosen plaintext security. Our scheme is constructed based on bilinear Diffie-Hellman inversion assumption and it is a good efficient hybrid encryption scheme, which achieves $O(1)$-size ciphertexts, public parameters and constant size private keys. In our scheme, either ciphertexts or public parameters has no relation with the number of receivers, moreover, both the encryption and decryption only require one pairing computation. Compared with other identity-based broadcast encryption schemes, our scheme has comparable properties, but with a better efficiency.**

***Index Terms*— Identity-based broadcast encryption, Random oracles, Bilinear Groups, Bilinear Diffie-Hellman Assumption**

I. INTRODUCTION

Broadcast encryption(BE) systems [1] allow a sender, who wants to send a message to a dynamically chosen subset $\mathcal{N} \subseteq [1, n]$ of users, to construct a ciphertext such that only users in $\mathcal{N}$ can decrypt; the sender can then safely transmit this ciphertext over a broadcast channel to all users. Many BE systems [2]–[6] have been proposed, and some of them make use of the hybrid encryption paradigm where the broadcast ciphertext only encrypts a symmetric key which is used to encrypt the broadcast contents. It is preferable if the system uses *public key* (anybody can encrypt), permits *stateless receivers* (users do not need to update their private keys), and is *fully collusion resistant* (even if all users outside of $\mathcal{N}$ collude, they cannot decrypt). Typically, we assume that a broadcast encryption system has these properties. For a useful secure broadcast system, short ciphertexts are required, thus the main challenge in building efficient broadcast systems is to encrypt messages with short ciphertexts.

The formal concept of the identity-based broadcast encryption (IBBE) was introduced by Delerablée in [7](and independently in [8]) in 2007. This concept is related to identity-based encryption(IBE) [9], in which the maximal size of a broadcast group is $\mathcal{N} = 1$. It is also related to multi receiver ID-based KEM (mID-KEM), introduced in [10] and further developed in [11]–[14].

In [7], Delerablée proposed the formal definition and security notions for IBBE. In his definition, an IBBE scheme basically includes an **Extract** procedure in the definition of Broadcast Encryption given in [5], and can also be viewed as a generalization of classical IBE systems. For security notions, Delerablée followed the definition of the classical security notions for BE (security against static adversaries), which is close to the notion of selective identity security(weaker than full security), used in [15]. Then, Delerablée proposed an IBBE scheme using a Key Encapsulation Mechanism (KEM), so that long messages can be encrypted under a short symmetric key. In his solution, ciphertexts and private keys are of constant size, and the public key is linear in the maximal value of $\mathcal{N}$. Finally, he proved that his construction is selective identity, chosen plaintext(IND-sID-CPA) secure. However, the security of his scheme requires cryptographic hash functions that are modeled as random oracles, i.e., his scheme is only proven secure in the random oracle model but maybe insecure in practice.

Recently, Guo [16] proposed an authority identity-based broadcast encryption(AA-IBBE) scheme based on the result of [7]. The scheme provides a new approach to mitigate the key escrow problem in IBBE schemes. In [16], Guo gave IND-sID-CPA security proof of his scheme in the random oracle model, but did not describe efficiency. Compared with the construction in [7], we assume that they have the same efficiency.

Moreover, in the year 2008, Boneh and Hamburg [17] developed a general framework for constructing identity-based encryption and broadcast encryption, and given the first broadcast hierarchical identity based encryption(HIBE) system with random oracles. The ciphertext size in all systems proposed in [17] is independent of the number of users involved, but private key size grows with the complexity of the system.

Lately, Gentry and Waters [21] presented new techniques for achieving adaptive security in broadcast encryption systems. Note that fully collusion resistant under adaptive attacks is the right model for security in broadcast encryption systems. In [21], they presented a new definition of security called semi-static security and showed a generic two-key transformation from semi-statically secure systems to adaptively secure systems that have comparable-size ciphertexts. Furthermore, they

doi:10.4304/jcp.5.3.331-336

presented the first adaptively secure IBBE scheme with public key of size $O(\lambda \cdot l)$ and constant-sized private keys(i.e., $O(\lambda)$).

In fact, the concept of the identity-based broadcast encryption was first introduced in [18] in 2003. Later, Du proposed an ID-based broadcast encryption scheme in [19] for key distribution, by which a center can distribute session keys to a certain set of users. A tiny difference from the scheme of [7] is that this scheme does not require a secure channel between each user and the center and only needs one round broadcast. In terms of efficiency, the communication transmission bandwidth of [19] is linearly dependent of the user size, the encryption requires one pairing computation but the decryption requires two pairing computation. Afterward, a new ID-based broadcast encryption scheme was proposed in [20] based on the result of [18], [19]. The new scheme has a good efficiency, both the encryption and decryption only require one pairing computation.

We focus on improving the security and efficiency based on the result of [7], and we have made the following contributions. We present a new efficient identity-based broadcasting encryption scheme that is IND-sID-CPA secure without random oracles. First, in our scheme, either the broadcast ciphertexts or the public key is $O(1)$-size and has no relation with the number of receivers. Second, the private keys used to decrypt by the receivers are of constant size. Third, the group manager can dynamically include new members while preserving previously computed information. In particular, user decryption keys need not be recomputed, the morphology and size of ciphertexts are unchanged and the group encryption key requires minimal or no modification. In short, our construction achieves $O(1)$-size ciphertexts, public key and constant size private keys, and it does not rely on random oracles.

II. Complexity Assumptions

Let $\mathcal{G}$ be a bilinear group of prime order p. We review the standard Bilinear Diffie-Hellman (BDH) assumption and describe the Bilinear Diffie-Hellman Inversion (BDHI) assumption.

A. Bilinear Groups

We briefly review the necessary facts about bilinear maps and bilinear map groups [9], [22]. We use the following notations:

1. $\mathcal{G}$ and $\mathcal{G}_1$ are two (multiplicative) cyclic groups of prime order p.
2. g is a generator of $\mathcal{G}$.
3. e is a bilinear map $e : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}_1$.

Let $\mathcal{G}$ and $\mathcal{G}_1$ be two groups as above. A bilinear map is a map $e : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}_1$ with the following properties:

1. Bilinearity: for all $u, v \in \mathcal{G}$ and $a, b \in \mathcal{Z}$, we have $e(u^a, v^b) = e(u, v)^{ab}$.
2. Non-degeneracy: $e(g, g) \neq 1$.

We say that $\mathcal{G}$ is a bilinear group if the group action in $\mathcal{G}$ can be computed efficiently and there exists a group $\mathcal{G}_1$ and an efficiently computable bilinear map $e : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}_1$ as above. Note that $e(\cdot, \cdot)$ is symmetric since $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

Throughout the paper, for a prime order group $\mathcal{G}$ we use $\mathcal{G}^*$ to denote the set $\mathcal{G} \setminus \{1_{\mathcal{G}}\}$ where $1_{\mathcal{G}}$ is the identity of $\mathcal{G}$.

B. Bilinear Diffie-Hellman Assumption

The BDH problem [9] in $\mathcal{G}$ is as follows: given a tuple $g, g^a, g^b, g^c \in \mathcal{G}$ as input, output $e(g, g)^{abc} \in \mathcal{G}_1$. An algorithm $\mathcal{A}$ has advantage ϵ in solving BDH in $\mathcal{G}$ if

$$\Pr[\mathcal{A}(g, g^a, g^b, g^c) = e(g, g)^{abc}] \geq \epsilon$$

where the probability is over the random choice of generator g in $\mathcal{G}^*$, the random choice of a, b, c in $\mathcal{Z}_p$, and the random bits used by $\mathcal{A}$. Similarly, we say that an algorithm $\mathcal{B}$ that outputs $b \in 0, 1$ has advantage ϵ in solving the *decision* BDH problem in $\mathcal{G}$ if

$$|\Pr[\mathcal{B}(g, g^a, g^b, g^c, e(g, g)^{abc}) = 0] - \Pr[\mathcal{B}(g, g^a, g^b, g^c, T) = 0]| \geq \epsilon$$

where the probability is over the random choice of generator g in $\mathcal{G}^*$, the random choice of a, b, c in $\mathcal{Z}_p$, the random choice of $T \in \mathcal{G}_1$, and the random bits consumed by $\mathcal{B}$. We refer to the distribution on the left as $\mathcal{P}_{BDH}$ and the distribution on the right as $\mathcal{R}_{BDH}$.

Definition 1. We say that (Decision)(t, ϵ)-BDH assumption holds in $\mathcal{G}$ if no t-time algorithm has advantage at least ϵ in solving the (Decision) BDH problem in $\mathcal{G}$. Occasionally we drop the t and ϵ and refer to the BDH and Decision BDH assumptions in $\mathcal{G}$.

C. Bilinear Diffie-Hellman Inversion Assumption

The q-BDHI problem is defined as follows: given the $(q + 1)$-tuple $(g, g^x, g^{(x^2)}, ..., g^{(x^q)}) \in (\mathcal{G}^*)^{q+1}$ as input, compute $e(g, g)^{1/x} \in \mathcal{G}_1^*$. An algorithm $\mathcal{A}$ has advantage ϵ in solving q-BDHI in $\mathcal{G}$ if

$$\Pr[\mathcal{A}(g, g^x, ..., g^{(x^q)}) = e(g, g)^{1/x}] \geq \epsilon$$

where the probability is over the random choice of generator g in $\mathcal{G}^*$, the random choice of the x in $\mathcal{Z}_p^*$, and the random bits of $\mathcal{A}$. Similarly, we say that an algorithm $\mathcal{B}$ that outputs $b \in \{0, 1\}$ has advantage ϵ in solving the *decisionq*-BDHI problem in $\mathcal{G}$ if

$$|\Pr[\mathcal{B}(g, g^x, ..., g^{(x^q)}, e(g, g)^{1/x}) = 0] - \Pr[\mathcal{B}(g, g^x, ..., g^{(x^q)}, T) = 0]| \geq \epsilon$$

where the probability is over the random choice of generator g in $\mathcal{G}^*$, the random choice of x in $\mathcal{Z}_p^*$, the random choice of $T \in \mathcal{G}_1$, and the random bits of $\mathcal{B}$. We refer to the distribution on the left as $\mathcal{P}_{BDHI}$ and the distribution on the right as $\mathcal{R}_{BDHI}$.

Definition 2. We say that the (Decision)(t, q, ϵ)-BDHI assumption holds in $\mathcal{G}$ if no t-time algorithm has advantage at least ϵ in solving the (Decision) q-BDHI problem in $\mathcal{G}$.

Occasionally we drop the t and ϵ and refer to the q-BDHI and Decision q-BDHI assumptions. It is not known

if the q-BDHI assumption, for $q > 1$, is equivalent to BDH. A closely related assumption was previously used in [23] where it was called weak Diffie-Hellman.

III. Formal Definition of IBBE

We follow the formal definition of IBBE, described in [7].

An IBBE scheme involves an authority: the Private Key Generator (PKG). The PKG grants new members capability of decrypting messages by providing each new member (with identity ID_i) a decryption key $\mathsf{sk}_{\mathsf{ID}_i}$. The generation of $\mathsf{sk}_{\mathsf{ID}_i}$ is performed using a master secret key MSK. An IBBE scheme with security parameter λ and maximal size m of the target set, is a tuple of algorithms $IBBE = (Setup, Extract, Encrypt, Decrypt)$ described as follows:

Setup(λ, m). Takes as input the security parameter λ and m the maximal size of the set of receivers for one encryption, and outputs a master secret key MSK and a public key PK. The PKG is given MSK, and PK is made public.

Extract(MSK, ID_i). Takes as input the master secret key MSK and a user identity ID_i. Extract generates a user private key $\mathsf{sk}_{\mathsf{ID}_i}$.

Encrypt($\mathcal{N}$,PK). Takes as input the public key PK and a set of included identities $\mathcal{N} = \{\mathsf{ID}_i, \cdots, \mathsf{ID}_n\}$ with $n \leq m$, and outputs a pair (Hdr, K), where Hdr is called the header, $K \in \mathcal{K}$ and $\mathcal{K}$ is the set of keys for the symmetric encryption scheme.

When a message $M \in \{0,1\}^*$ is to be broadcast to users in $\mathcal{N}$, the broadcaster generates $(\mathsf{Hdr}, K) \longleftarrow \mathrm{Encrypt}(\mathcal{N}, \mathsf{PK})$, computes the encryption C_M of M under the symmetric key K and broadcasts $(\mathsf{Hdr}, \mathcal{S}, C_M)$. We will refer to Hdr as the header or broadcast ciphertext, $(\mathsf{Hdr}, \mathcal{N})$ as the full header, K as the message encryption key and C_M as the broadcast body.

Decrypt($\mathcal{N}, \mathsf{ID}, \mathsf{sk}_{\mathsf{ID}}, \mathsf{Hdr}, \mathsf{PK}$). Takes as input a subset $\mathcal{N} = \{\mathsf{ID}_i, \cdots, \mathsf{ID}_n\}$ (with $n \leq m$), an identity ID and the corresponding private key $\mathsf{sk}_{\mathsf{ID}}$, a header Hdr, and the public parameters PK. If $\mathsf{ID} \in \mathcal{N}$, the algorithm outputs the message encryption key K which is then used to decrypt the broadcast body C_M and recover M.

Remark. This model defines, when $m = 1$, an IBE system.

IV. Security Notions for IBBE

Arguably, the "correct" definition for security in broadcast encryption systems is that of adaptive security. In an adaptively secure system, the adversary is allowed to see PK and then ask for several private keys before choosing the set of indices that it wishes to attack. Adaptive security in broadcast encryption is defined in [21] lately.

Our work began before the above definition was proposed, and security analysis was based on the weaker standard security notion described in [7]. One interesting open problem is constructing an efficient IBBE scheme without random oracles under the adaptive security notion.

The rest of this section is dedicated to describing the IND-sID-CPA security and IND-sID-CCA security for IBBE proposed in [7].

Security is defined using the following game between an adversary $\mathcal{A}$ and a challenger. Both the adversary and the challenger are given as input m, the maximal size of a set of receivers $\mathcal{N}$.

Init: The adversary $\mathcal{A}$ first outputs a set $\mathcal{N}^* = \{\mathsf{ID}_i^*, \cdots, \mathsf{ID}_n^*\}$ of identities that he wants to attack (with $n \leq m$).

Setup: The challenger runs Setup(λ ,m) to obtain a public parameters PK. He gives $\mathcal{A}$ the public key PK.

Query phase 1: The adversary $\mathcal{A}$ adaptively issues queries $q_1, \cdots, q_{n_0}$, where q_i is one of the following:

• Extraction query (ID_i) with the constraint that $\mathsf{ID}_i \notin \mathcal{N}^*$: The challenger runs Extract on ID_i and forwards the resulting private key to the adversary.

• Decryption query, which consists of a triple $(\mathsf{ID}_i, \mathcal{N}, \mathsf{Hdr})$ with $\mathcal{N} \in \mathcal{N}^*$ and $\mathsf{ID}_i \in \mathcal{N}$. The challenger responds with $\mathsf{Decrypt}(\mathcal{N}, \mathsf{ID}_i, \mathsf{sk}_{\mathsf{ID}i}, \mathsf{Hdr}, \mathsf{PK})$.

Challenge: When $\mathcal{A}$ decides that phase 1 is over, the challenger runs Encrypt algorithm to obtain $(\mathsf{Hdr}^*, K) = \mathsf{Encrypt}(\mathcal{N}^*, \mathsf{PK})$ where $K \in \mathcal{K}$. The challenger then randomly selects $b \leftarrow \{0,1\}$, sets $K_b = K$, and sets K_{1-b} to a random value in $\mathcal{K}$. The challenger returns $(\mathsf{Hdr}^*, K_0, K_1)$ to $\mathcal{A}$.

Query phase 2: The adversary continues to issue queries $q_{n_0+1}, \cdots, q_n$ where q_i is one of the following:

• Extraction query (ID_i), as in phase 1.

• Decryption query, as in phase 1, but with the constraint that $\mathsf{Hdr} \neq \mathsf{Hdr}^*$. The challenger responds as in phase 1.

Guess: Finally, the adversary $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$ and wins the game if $b = b'$.

We denote by $q_{_D}$ the total number of Decryption queries and by t the total number of extraction queries that can be issued by the adversary during the game. Viewing t, m, q_D as attack parameters, we denote by $\mathsf{Adv}^{\mathsf{ind}}_{\mathcal{IBBE}}(t, m, q_D, \mathcal{A})$ the advantage of $\mathcal{A}$ in winning the game:

$$\begin{aligned} & \mathsf{Adv}^{\mathsf{ind}}_{\mathcal{IBBE}}(t, m, q_D, \mathcal{A}) \\ = & \left| 2 \times \Pr[b = b^{'}] - 1 \right| \\ = & \left| \Pr[b = b^{'} | b = 1] - \Pr[b^{'} = 1 | b = 0] \right| \end{aligned}$$

where the probability is taken over the random coins of $\mathcal{A}$, the challenger and all probabilistic algorithms run by the challenger.

Definition 3. Let $\mathsf{Adv}^{\mathsf{ind}}_{\mathcal{IBBE}}(t, m, q_D, \mathcal{A}) = \max_{\mathcal{A}} \mathsf{Adv}^{\mathsf{ind}}_{\mathcal{IBBE}}(t, m, q_D, \mathcal{A})$ where the maximum is taken over all probabilistic algorithms $\mathcal{A}$ running in time $\mathsf{poly}(\lambda)$. An identity-based broadcast encryption scheme IBBE is said to be (t, m, q_D)-IND-sID-CCA secure if $\mathsf{Adv}^{\mathsf{ind}}_{\mathcal{IBBE}}(t, m, q_D) = \mathsf{negl}(\lambda)$.

IND-sID-CPA. We define semantic security for an IBBE scheme by preventing the attacker from issuing decryption queries.

Definition 4. We say that an identity-based broadcast encryption system is (t, m)-IND-sID-CPA secure if it is $(t, m, 0)$-IND-sID-CCA secure.

V. Our Construction

In this section, we present our IBBE scheme without random oracles based on the q-BDHI assumption. The proposed scheme achieves constant size ciphertexts, public key and private keys.

A. Basic Construction Description

Let $\mathcal{G}$ be a bilinear group of prime order p. We choose a cryptographic collision resistant hash function $H : \{0,1\}^* \rightarrow \mathcal{Z}_p^*$, which can map arbitrary identities as public keys (ID) in $\{0,1\}^*$ into $\mathcal{Z}_p^*$. We also assume the K to be encrypted is an element in $\mathcal{G}_1$, where $K \in \mathcal{K}$ and $\mathcal{K}$ is the set of keys for the symmetric encryption scheme.

Setup(λ, m): To generate the parameters of the IBBE system, given the security parameter λ and an integer m, a bilinear map group system $\mathcal{G} = (p, \mathcal{G}, \mathcal{G}_1, e(\cdot,\cdot))$ is constructed. We then select a random generator $g \in \mathcal{G}^*$, two random elements $x, y \in \mathcal{Z}_p^*$, and define $X = g^x$ and $Y = g^y$. The public key PK and the master secret key MSK are defined as follows:

$$\mathsf{PK} = (g, X, Y), \qquad \mathsf{MSK} = (x, y)$$

Extract$(\mathsf{MSK}, \mathsf{ID}_i)$: Now we have the $\mathsf{MSK} = (x, y)$, to create a private key for the public key identity $\mathsf{ID}_i \in \mathcal{Z}_p^*$:

1. pick a random element $r \in \mathcal{Z}_p$, and compute $R = g^{\frac{1}{(r+\mathsf{ID}_i)\cdot y + x}}$,
2. output the private key $\mathsf{sk}_{\mathsf{ID}_i} = (r, R)$.

In case of the unlikely event that $(r + \mathsf{ID}_i) \cdot y + x = 0 \pmod p$, try to select a new random value for r.

Encrypt$(\mathsf{PK}, \mathcal{N}, K)$: Assume the notation $\mathcal{N} = \{\mathsf{ID}_j\}_{j=1}^n$ represent the set of the receivers. To encrypt a symmetric encryption scheme's key $K \in \mathcal{K}$, the broadcaster needs to randomly pick a $s \in \mathcal{Z}_p^*$, and computes the $\mathsf{Hdr} = (A, B, C, D)$ using PK and s to encapsulate the symmetric key K, where

$$A = Y^{\prod_{j=1}^n \mathsf{ID}_j \cdot s} \qquad B = X^s$$
$$C = Y^s \qquad D = e(g,g)^s \cdot K$$

Note that $e(g, g)$ can be precomputed once for encryption everytime, so that it dose not require any pairing computations.

Decrypt$(\mathsf{PK}, \mathcal{N}, \mathsf{ID}_i, \mathsf{sk}_{\mathsf{ID}_i}, \mathsf{Hdr})$: In order to retrieve the message encryption key K encapsulated in the header $\mathsf{Hdr} = (A, B, C, D)$, the receiver in the set $\mathcal{N} = \{\mathsf{ID}_j\}_{j=1}^n$ with identity $\mathsf{ID}_i \in \mathcal{N} (1 \le i \le n)$ and the private key $\mathsf{sk}_{\mathsf{ID}_i} = (r, R)$ should compute and output $D/e(A^{1/(\prod_{j=1, j\neq i}^n \mathsf{ID}_j)} \cdot B \cdot C^r, R)$. Indeed, for the valid ciphertext we have

$$\begin{aligned} & \frac{D}{e(A^{\frac{1}{\prod_{j=1, j\neq i}^n \mathsf{ID}_j}} \cdot B \cdot C^r, R)} \\ = & \frac{D}{e(g^{y\cdot \mathsf{ID}_i \cdot s} \cdot g^{(x)\cdot s} \cdot g^{(y)\cdot s \cdot r}, g^{\frac{1}{(r+\mathsf{ID}_i)\cdot y + x}})} \\ = & \frac{e(g,g)^s \cdot K}{e(g,g)^s} = K \end{aligned}$$

B. Efficiency

In terms of efficiency, our construction achieves $O(1)$-size ciphertexts, public key and constant size private keys. We can get the result from the expressions of public key, private key and ciphertext as follows:

1. The expression of public key is $\mathsf{PK} = (g, X, Y)$, where $X = g^x$, $Y = g^y$ and $x, y \in \mathcal{Z}_p^*$. It is obvious that the public key is $O(1)$-size and has no relation with the number of receivers.

2. The expression of private key is $\mathsf{sk}_{\mathsf{ID}_i} = (r, R)$, where $r \in \mathcal{Z}_p$ and $R = g^{\frac{1}{(r+\mathsf{ID}_i)\cdot y + x}}$. It is obvious that the private key is constant size.

3. The expression of ciphertext is $\mathsf{Hdr} = (A, B, C, D)$:

$$A = Y^{\prod_{j=1}^n \mathsf{ID}_j \cdot s} \qquad B = X^s$$
$$C = Y^s \qquad D = e(g,g)^s \cdot K$$

where $s \in \mathcal{Z}_p^*$, K is the symmetric key. Because the result of $\prod_{j=1}^n \mathsf{ID}_j \cdot s$ is a numerical value, so the ciphertext has no relation with the number of receivers and it is $O(1)$-size.

Note that the public key in our construction is constant size which is different from the linear size of $\mathcal{N}$ in [7], [16], and shorter than the schemes in [21]; private keys is constant size which is different from growing with the complexity of the system in [17]; both the encryption and decryption only require one pairing computation, which is different from the number of pairing computation in [7], [16], [19]. As a result, our scheme has a better efficiency compared with other identity-based broadcast encryption schemes.

C. Security Analysis

We prove that our IBBE scheme without random oracles is selective identity, chosen plaintext(IND-sID-CPA) secure under the Decision q-BDHI assumption.

Theorem 1. *Suppose the (t, q, ϵ)-Decision BDHI assumption holds in $\mathcal{G}$ of size $|\mathcal{G}| = p$. Then the previously defined IBBE system is (t', q_D, ϵ)-selective identity, chosen plaintext*(IND-sID-CPA)*secure for any $q_D < q$, and any $t' < t - \Theta(\Gamma q^2)$ where Γ is the maximum time for an exponentiation in $\mathcal{G}$.*

Proof. The rest of this section is dedicated to proving Theorem 1. Suppose $\mathcal{A}$ has advantage ϵ in attacking the IBBE system. We build an algorithm $\mathcal{B}$ that uses $\mathcal{A}$ to solve the Decision q-BDHI problem in $\mathcal{G}$. Algorithm $\mathcal{B}$ is given as input a random $(q + 2)$-tuple $(g, g^\alpha, g^{\alpha^2}, ..., g^{\alpha^q}, T) \in (\mathcal{G}^*)^{q+1} \times \mathcal{G}_1$. Algorithm $\mathcal{B}$'s

goal is to output 1 if $T = e(g,g)^{1/\alpha}$ and 0 otherwise. Algorithm $\mathcal{B}$ works by interacting with $\mathcal{A}$ in a selective identity game as follows:

Preparation: Algorithm $\mathcal{B}$ builds a generator $h \in \mathcal{G}^*$ for which it knows $q-1$ pairs of the form $(w_i, h^{1/(\alpha \cdot w_i)})$ for random $w_1, w_2, ..., w_{q-2} \in \mathcal{Z}_p^*$. This is done as follows:

1. Pick random $w_1, w_2, ..., w_{q-2} \in \mathcal{Z}_p^*$ and let $f(z)$ be the polynomial $f(z) = \prod_{i=1}^{q-2}(z + w_i)$. Expand the terms of f to get $f(z) = \sum_{i=0}^{q-2} c_i z^i$. The constant term c_0 is non-zero.
2. Compute $h = \prod_{i=1}^{q-1} (g^{(\alpha)^i})^{c_{i-1}} = g^{\alpha f(\alpha)}$ and $u = \prod_{i=1}^{q-1} (g^{(\alpha)^{i+1}})^{c_{i-1}} = g^{\alpha^2 f(\alpha)}$. Note that $u = h^\alpha$.
3. Check that $h \in \mathcal{G}^*$. Indeed if we had $h = 1$ in $\mathcal{G}$ this would mean that $w_j = -\alpha$ for some easily identifiale w_j, at which point $\mathcal{B}$ would be able to solve the challenge directly. Thus we assume that all $w_j \neq -\alpha$.
4. Observe that for any $i = 1, ..., q-2$, it is easy for $\mathcal{B}$ to construct the pair $(w_i, h^{1/(\alpha \cdot w_i)})$. To see this, we have

$$f_i(z) = \frac{\alpha f(z)}{\alpha w_i} = \frac{f(z)}{w_i} = \sum_{j=0}^{q-2} \frac{c_j}{w_i} z^j = \sum_{j=0}^{q-2} d_j z^j$$

Then

$$h^{\frac{1}{\alpha \cdot w_i}} = g^{f_i(\alpha)} = \sum_{j=0}^{q-2} (g^{(\alpha^j)})^{d_j}$$

5. Afterward, $\mathcal{B}$ computes

$$T_h = T^{c_0^2} \cdot T_0$$

where

$$T_0 = \prod_{i=0}^{q-2} \prod_{j=0}^{q-3} e(g^{(\alpha)^i}, g^{(\alpha)^j})^{c_i c_{j+1}}$$

Observe that if $T = e(g,g)^{1/\alpha}$ then $T_h = e(g^{f(\alpha)/\alpha}, g^{f(\alpha)}) = e(h,h)^{1/\alpha}$. On the contrary, if T is uniform in $\mathcal{G}_1$, then so is T_h.

We will be using the values h, u, T_h and the pairs $(w_i, h^{1/(\alpha \cdot w_i)})$ for $i = 1, ...q-1$ throughout the simulation.

Initialization: The selective identity game begin with the adversary $\mathcal{A}$ first outputting a set $\mathcal{N}^* = \{\mathsf{ID}_j^*\}_{j=1}^n$of identities he wants to attack.

Setup: To generate the system parameters, Algorithm $\mathcal{B}$ dose the following:

1. Pick random $a \in \mathcal{Z}_p^*$ and let $b = \prod_{j=1}^n \mathsf{ID}_j^*$.
2. Compute $X = u^{a+b} = h^{\alpha(a+b)}$ and $Y = u = h^\alpha$.
3. Publish $\mathsf{PK} = (h, X, Y)$ as the public key, Note that the X, Y are independent of ID_j^* in the adversary's view.
4. We implicitly define $x = \alpha(a+b)$ and $y = \alpha$, so that $X = h^x$ and $Y = h^y$. Algorithm $\mathcal{B}$ dose not know the value of x and y.

Phase 1: The adversary $\mathcal{A}$ issues up to $q_D < q-1$ private key queries. Consider the i-th query for the private key corresponding to public key $\mathsf{ID}_i \notin \{\mathsf{ID}_j^*\}_{j=1}^n$. We need to respond with a private key $(r, h^{\frac{1}{(r+\mathsf{ID}_i)\cdot y + x}})$ for a uniformly distributed $r \in \mathcal{Z}_P$. Algorithm $\mathcal{B}$ responds to the query as follows:

1. Let$(w_i, h^{1/(\alpha \cdot w_i)})$ be the i-th pair constructed during the preparation step. Define $h_i = h^{1/(\alpha \cdot w_i)}$
2. $\mathcal{B}$ first constructs an $r \in \mathcal{Z}_p$ satisfying $(r + a + b) \cdot \alpha w_i = (r + \mathsf{ID}_i) \cdot y + x$. Plugging in the values of x and y the equation becomes

$$(r + a + b) \cdot \alpha w_i = (r + \mathsf{ID}_i) \cdot \alpha + \alpha(a+b)$$

we see that the unknown α cancels from the equation and we get $r = \frac{\mathsf{ID}_i}{w_i - 1} - (a+b) \in \mathcal{Z}_p$ which $\mathcal{B}$ can evaluate.
3. Now , $(r, h^{\frac{1}{r+a+b}})$ is a valid private key for ID_i, for

$$h_i^{\frac{1}{r+a+b}} = (h^{\frac{1}{\alpha w_i}})^{r+a+b} = h^{\frac{1}{(r+\mathsf{ID}_i)\cdot y + x}}$$

as required. From the construction of r we can see that it is uniformly distributed among all elements in $\mathcal{Z}_p$ for which $(r+\mathsf{ID}_i)\cdot y + x \neq 0$ and $r \neq -(a+b)$.

Challenge: The adversary $\mathcal{A}$ outputs two message $M_0, M_1 \in \mathcal{G}_1$, algorithm $\mathcal{B}$ picks a random bit $b \in \{0,1\}$ and a random $\ell \in \mathcal{Z}_p^*$. It responds with the ciphertext $CT = (h^{b\cdot\ell},\ h^{(a+b)\cdot\ell},\ h^\ell,\ T_h^\ell \cdot M_b)$. Define $s = \ell/\alpha$. On the other hand, if $T_h = e(g,g)^{1/\alpha}$ we have

$$h^{b\cdot\ell} = h^{\prod_{j=1}^n \mathsf{ID}_j^* \cdot \ell} = h^{\alpha \cdot \prod_{j=1}^n \mathsf{ID}_j^* \cdot s} = Y^{\prod_{j=1}^n \mathsf{ID}_j^* \cdot s}$$

$$h^{(a+b)\cdot\ell} = h^{\alpha\cdot(a+b)\cdot s} = (h^x)^s = X^s$$

$$h^\ell = h^{\alpha \cdot s} = Y^s$$

It follows that CT is a valid encryption of M_b under ID^*, with the uniformly distributed randomization value $s = \ell/\alpha \in \mathcal{Z}_p^*$. On the other hand when T_h is uniform in $\mathcal{G}_1$, then , in the adversary's view, CT is independent of the bit b.

Phase 2: The adversary $\mathcal{A}$ issues more private key queries, for a total of at most $q_D < q-1$. Algorithm $\mathcal{B}$ responds as before.

Guess: Finally, $\mathcal{A}$ outputs a guess $b' \in \{, 0, 1\}$. If $b = b'$ then $\mathcal{B}$ outputs 1 meaning $T = e(g,g)^{1/\alpha}$. Otherwise, it outputs 0 meaning $T \neq e(g,g)^{1/\alpha}$.

We show that when the input tuple is sampled from $\mathcal{P}_{BDHI}$(where $T = e(g,g)^{1/\alpha}$) then $T_h = e(h,h)^{1/\alpha}$ in which case $\mathcal{A}$ must satisfy $|\Pr[\mathrm{b} = \mathrm{b}'] - 1/2| > \epsilon$. On the other hand, when the input tuple is sampled from $\mathcal{R}_{BDHI}$(Where T is uniform in $\mathcal{G}_1$) then T_h is uniform and independent in $\mathcal{G}_1$ in which case $\Pr[\mathrm{b} = \mathrm{b}'] = 1/2$. Therefore, with g uniform in $\mathcal{G}^*$, x uniform in $\mathcal{Z}_p^*$ and T uniform in $\mathcal{G}_1$, we have that

$$|\Pr[\mathcal{B}(g, g^x, ..., g^{(x^q)}, e(g,g)^{1/x}) = 0] - \Pr[\mathcal{B}(g, g^x, ..., g^{(x^q)}, T) = 0]| \geq |(\frac{1}{2} \pm \epsilon) - \frac{1}{2}| \geq \epsilon$$

as required.

This completes the proof of the Theorem 1.

The proof process is similar with [15].

VI. Conclusion

The paper constructs an identity-based broadcast encryption scheme which does not use the cryptographic hash functions that are modeled as random oracles. We then prove that it is a selective identity, chosen plaintext secure scheme.

In terms of efficiency, the scheme achieves $O(1)$-size ciphertexts, public key and constant size private keys, either ciphertexts or public key has no relation with the number of receivers, and both the encryption and decryption only require one pairing computation. Moreover, the total number of possible users does not have to be fixed in the setup in our scheme.

In terms of security, the construction is based on the selective identity security notion, but lately, a strong standard notion has been proposed in [21], one open problem would be constructing an adaptively secure efficient IBBE scheme which does not rely on the random oracles under some standard decision assumptions.

Acknowledgment

The authors are grateful for the support given by National Natural Science Foundation of China (Grant No. 60473099, Grant No. 60873235). We also thank reviewers for insightful comments and helpful suggestions.

References

[1] Amos Fiat and Moni Naor. Broadcast encryption. In CRYPTO'93, LNCS 773, pp. 480-491, 1994.
[2] Dalit Naor, Moni Naor, and Jeffery Lotspiech. Revocation and tracing schemes for stateless receivers. In CRYPTO 2001, LNCS 2139, pp. 41-62, 2001.
[3] Dani Halevy and Adi Shamir. The CRYPTO 2002, LNCS 2442, pp. 47-60, 2002.
[4] Michael T. Goodrich, Jonathan Z. Sun, and Roberto Tamassia. Efficient treebased revocation in groups of low-state devices. In CRYPTO 2004, LNCS 3152, pp. 511-527, 2004.
[5] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In CRYPTO 2005, LNCS 3621, pp. 258-275, 2005.
[6] Cćile Delerablée, Pascal Paillier, and David Pointcheval. Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In PAIRING 2007, LNCS 4575, pp. 39-59, 2007.
[7] Cćile Delerablée. Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. In ASIACRYPT 07, pp. 200-215, 2007.
[8] Ryuichi Sakai and Jun Furukawa. Identity-Based Broadcast Encryption. In Eprint 2007/217, 2007.
[9] Dan Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In CRYPTO 2001, LNCS 2139, pp. 213-229, 2001.
[10] Nigel P. Smart. Efficient key encapsulation to multiple parties. Security in Communication Networks, LNCS 3352, pp. 208-219, 2005.
[11] Manuel Barbosa and P. Farshim. Effcient identity-based key encapsulation to multiple parties. In IMA Int. Conf., LNCS 3796, pp. 428-441, 2005
[12] Joonsang Baek, Reihaneh Safavi-Naini, and Willy Susilo. Effcient multi-receiver identity-based encryption and its application to broadcast encryption. In PKC 2005, LNCS 3386, pp. 380-397, 2005.
[13] Sanjit Chatterjee and Palash Sarkar. Multi-receiver identity-based key encapsulation with shortened ciphertext. In INDOCRYPT 2006, LNCS 4329, pp. 394-408, 2006.
[14] Michel Abdalla, Eike Kiltz and Gregory Neven. Generalized Key Delegation for Hierarchical Identity-Based Encryption. In ESORICS 07, LNCS 4734, pp. 139-154, 2007.
[15] Dan Boneh and Xavier Boyen. Efficient selective-ID secure identity based encryption without random oracles. In Advances in Cryptology-EUROCRYPT 2004, LNCS 3027, pp. 223-238, 2004.
[16] Shanqing Guo, Chunhua Zhang. Identity-based Broadcast Encryption Scheme with Untrusted PKG. In ICYCS 2008, pp. 1613-1618, 2008.
[17] Dan Boneh, Michael Hamburg. Generalized Identity Based and Broadcast Encryption Schemes. In ASIACRYPT 2008, LNCS 5350, pp. 455-470, 2008.
[18] Mu, Y., Susilo1, W., Lin, Y.X.: Identity-Based Broadcasting. INDOcrypto03. Lecture Notes in Computer Science, Vol. 2904. pp. 177-190, 2003.
[19] X. Du, Y.Wang, J. Ge, and Y.Wang. An ID-based broadcast encryption scheme for key distribution. In IEEE Transactions on Broadcasting , vol.51, no.2, pp. 264-266, June 2005.
[20] Chen Yang, Xiangguo Cheng, Wenping Ma, and Xinmei Wang. a new ID-based broadcast encryption scheme. In ATC 2006, LNCS 4158, pp. 487-492, 2006.
[21] Craig Gentry, Brent Waters. Adaptive Security in Broadcast Encryption Systems. Accepted by EUROCRYPT 2009, available at http://eprint.iacr.org/2008/268, 2009.
[22] Antoine Joux. A one round protocol for tripartite Diffie-Hellman. In Proceedings of ANTS IV, LNCS 1838, pp. 385-394, 2000.
[23] S.Mitsunari, R.Sakai, and M.Kasahara. A new traitor tracing. In IEICE Transactions on Fundamentals. E85-A(2), pp. 481-484, 2002.

Liang Hu Dr Liang Hu had his BEng on Computer Systems Organization in 1993 and his PhD on Computer Software and Theory in 1999. He is currently Professor and PhD supervisor of College of Computer Science and Technology, Jilin University, China.

His main research interests include distributed systems, computer networks, communications technology and information security system, etc. As a person in charge or a principal participant, Dr Liang Hu has finished more than 20 national, provincial and ministerial level research projects of China.

Zheli Liuwas born in 1978. He had his BSc and MSc in Computer Science from the Jilin University, China, in 2002 and 2005 respectively. Since 2005, he has been a PhD degree candidate in computer science from the Jilin University. His current interests include information security, cryptography, identity based encryption.

Xiaochun Cheng Dr Xiaochun Cheng had his BEng on Computer Software in 1992 and his PhD on Artificial Intelligence in 1996. He has been a senior member of IEEE since 2004. He is the secretary for IEEE SMC UK&RI. He is a member of IEEE SMC: Technical Committee on Systems Safety and Security. He is also a committee member of European Systems Safety Society.